Exhibit 3 to Appendix D to Contract No. DIR-TSO-3793
SaaS Module
US Public Sector (Direct)

1. INTRODUCTION

1.1. This Module for Software as a Service ("SaaS Module") between CA, Inc., located at 520 Madison Avenue, 22nd Floor, New York, NY 10022 ("CA"), and _____, located at _____ ("Customer"), effective _____ specifies terms and conditions which apply to SaaS that CA will provide to Customer.

1.2. This SaaS Module and DIR-TSO-3793 and the Foundation Agreement, effective _____ between CA and the Customer set forth the terms and conditions under which Customer may utilize SaaS. This SaaS Module incorporates by reference the terms of the Foundation Agreement, effective _____ between CA and Customer. Any capitalized terms used in this SaaS Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITIONS

2.1. "Authorized Use Limitation" means the limitation on usage of SaaS as measured by the Billing Metric specified in the Transaction Document.

2.2. "Authorized Users" means Customer, its employees and independent contractors and/or its Affiliates or as otherwise defined in the SaaS Listing, that access and use SaaS provided that they are bound by terms and conditions no less restrictive than those contained in the Agreement and solely to the extent that they are acting on behalf of Customer or its Affiliates.

2.3. "Billing Metric" means the metric for billing SaaS to Customer as defined in the SaaS Listing (*e.g.*, users, transactions, etc.).

2.4. "Customer Data" means any information provided by Authorized Users in the course of accessing and using SaaS and stored in connection with SaaS.

2.5. "Data Center Region" means a geographic region that are served by one or more hosting facilities for CA SaaS. CA Data Center Regions are: Americas, EMEA (Europe, Middle East, Asia) and APJ (Asia-Pacific, Japan).

2.6. "Force Majeure Event" means an event that arises out of causes beyond a Party's reasonable control, including, without limitation, war, civil commotion, act of God, strike or other stoppage (whether partial or total) of labor, any law, decree, regulation or order of any government or governmental body (including any court or tribunal) and/or delays or outages caused by an internet service provider or independent (not a Party's subcontractor) hosting facility.

2.7. "Non-Production" means any Customer deployed environment that is not Production such as development, test, staging, demonstration, or training environments.

2.8. "Production" means the "live" environment of SaaS that Customer uses as their primary business environment.

2.9. "SaaS" or "SaaS Offering" means the online version of the CA software and/or type of online service defined in the Transaction Document and made available to Authorized Users via the Internet.

2.10. "SaaS Listing" means the operating parameters, data and data center location(s), applicable audit standards, availability standards and any other details for the specific SaaS Offering as published or made available by CA. SaaS Listings may define provisioning and management processes applicable to the SaaS Offering, types and quantities of system resources (such as storage allotments), functional and technical aspects of the SaaS, as well as a catalogue of available service requests. These listings are available at http://www.ca.com/us/lpg/saas-knowledge-is-power.aspx

2.11. "SaaS Support" means support of the SaaS Offering so it operates materially in accordance with the Documentation.

2.12. "SaaS Release and Upgrade Policy" means CA's published policy on version and patch upgrades of its SaaS Offerings. This SaaS Release and Upgrade Policy can be found at http://www.ca.com/us/lpg/saas-knowledge-is-power.aspx.

2.13. "Scheduled Downtime" means planned downtime of SaaS availability for periodic and required maintenance events, including but not limited to, upgrades and updates to the SaaS and data center infrastructure where CA provides notice to Customer at least 72 hours in advance.

2.14. "Service Level Availability" or "SLA" means the targeted availability levels measured in the Production environment, as specified in the SaaS Listing which may vary according to each SaaS Offering and its component capabilities.

2.15. "Security Breach" means access to Customer Data by an unauthorized person or entity.

2.16. "Subscription Term" means the initial or renewal period of the subscription to a SaaS Offering as set out in the Transaction Document.

2.17. "Trial Period" means the period of time that Customer accesses and uses SaaS for evaluation or trial set out in the Transaction Document. If no time is indicated, then the period shall be set for thirty (30) days from the effective date of the Transaction Document. For avoidance of doubt, only a Transaction Document which explicitly states that it is for trial or evaluation by the Customer shall be considered a trial use.

2.18. "Transaction Document" means a signed mutually agreed ordering document such as a CA order form or statement of work for the specific CA offering licensed or purchased.

3. SAAS OFFERING

3.1. CA provides Customer a non-transferable and non-exclusive right for Customer and its Authorized Users to access and use SaaS during the Subscription Term in accordance with the Agreement.

3.2. Customer acknowledges and agrees that in order for Customer to access and use SaaS, Customer is required to maintain minimum requirements such as operating system versions, browsers etc., as stated in the Documentation. If required, information about updates to minimum requirements will be provided to Customer during the Subscription Term.

3.3. If CA provides software to Customer to enable or to optimize SaaS during the Subscription Term, such software will be listed in the Transaction Document. Such software is specifically provided to Customer to help Customer utilize certain applications and web services that may be available through SaaS. In such cases, CA provides Customer, during the Subscription Term, a non-transferable and non-exclusive right to use such software solely in connection with SaaS and for the sole purpose of allowing Customer's applications or web services to utilize SaaS. The grant of rights for such software is contingent upon Customer's compliance with the following obligations: Customer agrees, that neither it nor Authorized Users shall: (i) access or use any portion of the software not expressly authorized in the Transaction Document or the Documentation; (ii) cause or permit de-compilation, reverse engineering, or otherwise translate all or any portion of the software; (iii) modify, unbundle, or create derivative works of the software and/or Documentation; (iv) rent, sell, lease, assign, transfer or sublicense the software or use the software to provide hosting, service bureau, on demand or outsourcing services for the benefit of a third party; (v) remove any proprietary notices, labels, or marks on or in any copy or version of the software or Documentation; (vi) use the software beyond the rights granted. Any installation of agents or software of any kind will be required to be removed at the end of the Subscription Term and either returned to CA or Customer will be required to certify destruction or deletion of such items.

3.4. If SaaS is provided on a trial basis, Customer agrees to access and use SaaS solely for trial and evaluation purposes during the Trial Period, in accordance with the usage restrictions set forth in the Transaction Document. At the end of the Trial Period, Customer's right to access and use SaaS automatically expires and Customer agrees to cease accessing and using SaaS and to de-install any agents or copies of software provided as part of the SaaS and certify to CA in writing that all copies or partial copies of any such software have been deleted from Customer's computer libraries and/or storage devices and destroyed. If Customer desires to continue its use of SaaS beyond the Trial Period, Customer may enter into a Transaction Document and pay the applicable fees. DURING TRIAL PERIODS, CUSTOMER AGREES TO ACCESS AND USE SUCH SAAS ON AN AS IS BASIS AND AGREES THAT CA PROVIDES NO WARRANTIES, SLAS OR INDEMNITIES ARISING OUT OF SUCH ACCESS AND USE. ANY DATA ENTERED OR CONFIGURATION OF THE SAAS DURING THE TRIAL PERIOD WILL NOT BE STORED OR AVAILABLE AFTER THE TRIAL PERIOD.

4. FEES, RENEWAL & TERMINATION

4.1. The Authorized Use Limitation and associated fees shall be as set out on the Transaction Document. Unless otherwise stated, CA will monitor Customer's SaaS usage. In the event Customer exceeds the Authorized Use Limitation, the overage will be treated as an order for excess use and Customer will be billed for the overage at the rates stated in the applicable Transaction Document. The overage will be included in the Authorized Use Limitation for the remainder of the Subscription Term. Customer agrees that the purchase of any SaaS is not contingent on CA providing any future features or functionalities. In addition, Customer may order any service catalogue items which may be listed on the applicable Transaction Document or on the CA Support site (http://support.ca.com) ("CA Support Site") and by: entering into a separate Transaction Document for same; opening a ticket on the CA Support Site; submitting an order at the site listed on the Transaction Document, and/or if applicable; enter into an agreement for professional services. Customer shall pay any associated fees arising out of any such order.

4.2. Any Subscription Term may be renewed upon at least ninety (90) days prior to the expiration of the Subscription Term written notice by Customer subject to the renewal fees indicated on the Transaction Document or otherwise the then current subscription SaaS fees apply. Expiration or termination of any particular SaaS Offering shall not impact the validity of any other SaaS Offering Customer may be subscribing to.

4.3. Data availability, retention and destruction post expiration or termination of the applicable SaaS Offering will be as follows:

I. Customer Data will be available to Customer during the Subscription Term and may be retained by CA for a period of no more than sixty (60) days from the effective date of expiration or termination.

II. Subject to Appendix A, Section 9, C, of the DIR Contract No. DIR-TSO-3793, a record of Customer Data required to support audits of the billing transactions that occurred during the Subscription Term will be retained in accordance with CA's data retention policies for such activities and in accordance with the Agreement, including, without limitation, Article 6 (Security) of this SaaS Module. All other Customer Data will be deleted from all Production and Non-Production Environments within sixty (60) days of such date.

4.4. CA may temporarily suspend any Customer account, and/or a Customer's access to or use of the SaaS if the Authorized Users violate any provision within the "SaaS Offering" "Customer Data" or "Customer Responsibilities" sections of this Agreement, or if in CA's reasonable judgment, the SaaS services or any component thereof are about to suffer a significant threat to security or stability based on any unauthorized use. CA will provide Customer advance notice of any such suspension in CA's reasonable discretion based on the nature of the circumstances giving rise to the suspension. CA will use reasonable efforts to re-establish the affected SaaS services promptly after CA determines, in its reasonable opinion, that the situation giving rise to the suspension has been cured; however, after any suspension period, CA will make available to Customer the Customer Data and SaaS as existing in the Production environment on the date of suspension. CA or Customer may terminate the SaaS services under an order if any of the foregoing causes of suspension is not cured within 30 days after CA's initial notice thereof. Any suspension or termination by CA under this paragraph shall not excuse Customer from its obligation to make payment(s) under this Agreement.

5. CUSTOMER DATA

5.1. Customer exclusively owns all rights, title and interest in and to all Customer Data which may include personally identifiable information. Customer Data shall be considered to be Confidential Information under the Agreement. Customer Data will be stored and processed in the Data Center Region specified in the SaaS Listing. CA shall not access Customer's user accounts, or Customer Data, except (i) in the course of data center business operations if required, (ii) in response to SaaS or technical issues, or (iii) at Customer's specific request as reasonably required in the provision and support of SaaS.

5.2. CA runs security background checks on all production operation staff who may have access to Customer Data. Security audits, as specified in the SaaS Service Listing, are conducted periodically to certify that security controls are in place and background checks have been conducted.

CA may utilize subcontractors in the provision of SaaS Services so long as such subcontractors are bound to contractual terms no less protective of Customer's rights provided hereunder and provided further that any use of subcontractors in the operation of any applicable data center is subject to the same security controls and audits as if performed by CA employees. The Parties understand and agree that CA remains fully liable under the terms of the Agreement for any breach caused by a subcontractor of CA.

5.3. CA will collect, modify and analyse meta data and/or operations data which does not contain any Customer Data, such as system log files and transaction counts which relate to system utilization and performance statistics, all as deemed necessary by CA.

5.4. Customer may access reports and/or information through SaaS until the end of the Subscription Term. All reports and other output will be produced in standard readable format (*e.g.*, CSV, XML) and transmitted according to the transmission protocols used by the SaaS Offering for such transmissions. Any specific reports or data requested by Customer at the end of the Subscription Term that is not available through SaaS or produced in customized formats will be charged based on the scope of the request. Such fees will be agreed in writing between Customer and CA.

5.5. In case of a Force Majeure Event, Customer acknowledges and agrees that Customer Data may not be fully recoverable beyond the last restoration archive point, the frequency of which is described in the SaaS Listing.

5.6. **Customer agrees not to provide any health, payment card or similarly sensitive personal information that imposes specific data security obligations for the processing of such data part unless it is a supported feature in the Documentation of the applicable SaaS Offering.**

6. SECURITY

6.1. CA will maintain and administer a security policy with physical and technical safeguards designed to protect the security, integrity and confidentiality of the Customer Data. CA shall adhere to and subject such policies and practices to an audit under the compliance criteria defined in the applicable SaaS Listing. Upon written request, Customer may review the specific audit reports (such as SSAE 16 report) subject to Customer designating a security officer or similar individual who has executed a security non-disclosure agreement with CA prior to such review.

6.2. CA will not be responsible for any unauthorized access, alteration, theft or destruction of Customer Data, unless caused as a result of CA's negligence or intentional misconduct, in which case CA's only obligation and Customer's exclusive remedy is for CA to use commercially reasonable efforts to restore the Customer Data from the most recent back-up. CA is not responsible for unauthorized access, alteration, theft or destruction of Customer Data arising from Customer's own or its Authorized Users' actions or omissions in contravention of the Documentation.

6.3. CA shall comply with the applicable European Union member states' implementation of the Directive 95/46/EC ("Directive") governing the processing of personal data as defined in the Directive. CA, Inc. is Safe Harbour certified and will continue with this program whilst it is available or until CA adopts another legally recognized vehicle for such data transfers. At all times, all Customer Data shall remain within the continental United States unless provided otherwise in the Transaction Document.In the event that CA has determined that a Security Breach will or is likely to cause harm to the Customer or an Authorized User, CA will, within 24 HOURS, provide Customer with notice of the Security Breach. After initial notification, CA will keep Customer updated at periodic intervals on the steps taken by CA to investigate the Security Breach including providing a reasonably detailed incident report, including measures to be taken by the Customer to minimize potential damages. Such report will be provided promptly but no later than thirty (30) days following completion of the report. The Parties understand and agree that if CA is prevented by law or regulation from providing such notice(s) and/or reports within the time frames, such delay shall be excused.

6.4. Subject to Appendix A, Section 9, C, of the DIR Contract No. DIR-TSO-3793, during the Subscription Term, CA will permit Customer through an independent third party agreed in advance with CA, to audit CA's SaaS operations within the applicable data center the SaaS Offering is provided to Customer, solely to verify CA's compliance with the SaaS Listing concerning security and solely at Customer's expense. Any such audit shall be conducted not more than once annually, upon at least thirty (30) days prior written notice and subject to the independent third party having executed a non-disclosure agreement with CA stating the purpose and scope of the request. Such audit shall be conducted during normal business hours in a manner that does not disrupt business operations. In the event an external audit determines that CA fails to meet the standards defined in the SaaS Listing, CA will review and if it agrees with such determination it will have the opportunity to submit a plan to address any issues and CA will do so within thirty (30) days from receipt of notice from the Customer, or if CA does not agree with the determination the Parties will enter into discussions to resolve the issues. If audits require time and operations interruption, then Customer may be required to pay for costs and expenses as mutually agreed by the Parties. CA acknowledges that this paragraph in no way limits the rights and powers of the State Auditor's Office, and CA's obligations in relation to the State Auditor's Office, that result from CA's contracting with DIR and/or Customer.

7. SAAS SUPPORT

7.1. Upon the start of the Subscription Term, CA will send an email to Customer's technical contact, identified on the Transaction Document, providing information to connect and access SaaS and SaaS Support.

7.2. The Customer shall be provided with SaaS Support during the Subscription Term in accordance with CA's Support Policies at support.ca.com. To access SaaS Support, Customer may utilize the CA support website, or other site or notification mechanism as CA may designate from time to time.

7.3. Access to SaaS Support is limited to supported versions of the SaaS Offerings, as per the SaaS Upgrade Policy. Extended support agreements for non-supported versions of SaaS Offerings are not offered.

7.4. For any SaaS Support requests, Customer should be prepared to provide to support personnel all pertinent information, in English, including but not limited to, Customer number or site identification number, incident severity, SaaS Offering, SaaS environment (Production or Non-Production), incident description, and a technical contact familiar with Customer's environment or the problem to be solved. Customer must use reasonable efforts to communicate with CA in order to verify the existence of the problem and provide information about the conditions under which the problem could be re-created.

7.5. Upon receiving Customer's technical contact information, SaaS Support will be provided in a timely and professional manner by qualified support engineers. SaaS Support shall consist of:

i. Access to CA support website (currently: http://support.ca.com) for 24x7x365 online support and access to CA software product and Documentation, incident severity description with response and resolution objectives listed, global user communities and regional user groups, Frequently Asked Questions, samples, webcast recordings and demos, usage tips, technical updates and HYPER notifications, as such are made available by CA.

ii. Access to CA help desk and the ability to open and manage support incidents via CA support online or by telephone.

iii. Production environment support: 24x7 for severity 1 incidents; normal business hours for severities 2- 4.

iv. If applicable to the SaaS Offering, Non-Production environment support: Normal business hours for incidents of all severities.

v. Interactive remote diagnostic support allowing CA support engineers to troubleshoot an incident securely through a real-time browser-based remote control feature for support issues which may be resident in Customer's software or systems.

7.6. Additional support such as file storage, point in time backup, periodic file refresh and basic reporting may be available at CA's discretion according to the type of SaaS Offering provided and where indicated on the Transaction Document or in the SaaS Listing. Any additional support requirements are by prior written agreement of CA.

7.7. During the Subscription Term, if Customer requests specific scripts, connectors or customizations in order to optimize usage of SaaS, Customer may request CA to provide such services. Such services will be provided through a professional services agreement with CA for a separate fee, or as mutually agreed by the Parties.

8. MAINTENANCE AND UPGRADES

8.1. CA may update, improve, modify or add new functionality to SaaS during the Subscription Term for optimization of SaaS as necessary in order to maintain performance and/or fix any issues during the Subscription Term. In the event any update will materially change either the administrator or user experience, CA will provide Customer reasonable prior notice (not less than 30 days) and will provide a preview site where Customer can observe such changes where applicable, provided however, that CA may make a change with shorter or no notice if the change is required by law or to fix a security vulnerability.

8.2. CA may make changes or updates to the SaaS infrastructure (such as compute infrastructure, storage technology, security, technical configurations, hosting facilities within Data Center Region, etc.) during the Subscription Term, including to reflect changes in technology, industry practices, patterns of system use.

8.3. Customer is obligated to stay current on a supported version of the SaaS Offering, as per the SaaS Release and Upgrade Policy.

9. CUSTOMER RESPONSIBILITIES

9.1. Customer is responsible for all activities that occur in, or are related to, user accounts including the data, information stored or transmitted when accessing SaaS. All applications residing within Customer environment or installed on 3rd party service providers on behalf of Customer that integrate to SaaS shall be managed and supported by Customer. Customer is also responsible for managing components that are downloaded onto their environment such as web browser based software plug-ins that extend SaaS.

9.2. As Customer may integrate or utilize third party links to other software, hardware or other services which are associated with, or otherwise available through the SaaS, Customer agrees that it and/or its Affiliates, its Authorized Users and anyone acting on their behalf shall use such third party links at their sole discretion. CA shall have no responsibility or liability with respect to such third party links used by Customer's and/or its Affiliates, its Authorized Users or for any act or omission of any such third party provider.

9.3. Customer shall not: (i) make SaaS available to any third party not authorized or as otherwise contemplated by the Agreement; (ii) send or store code that can harm or result in damage to SaaS (including but not limited to malicious code and malware); (iii) wilfully interfere with or disrupt the integrity of SaaS or the data contained therein; (iv) attempt to gain unauthorized access to the SaaS or its related system or networks; (v) use SaaS to provide services to third parties except as expressly permitted by the Agreement; (vi) use SaaS in order to cause harm such as overload or create multiple agents for the purpose of disrupting operations of a third party; (vii) remove or modify any program markings or any notice CA's or its licensors' proprietary rights; (viii) perform or disclose any benchmark or performance tests on the SaaS; or (ix) perform or disclose any of the following security testing of the SaaS environments or associated infrastructure: network discovery, port and service identification, vulnerability scanning, password cracking, remote access testing, penetration testing or any other test or procedure not authorized in the Documentation. A breach by the Customer of its obligations under this section shall be considered a material breach of the Agreement.

10. WARRANTY

10.1. CA warrants that during the Subscription Term, the SaaS shall perform materially in accordance with the applicable Documentation subject to Customer's compliance with the Agreement. During any Trial Period, this warranty shall not apply.

10.2. EXCEPT AS EXPRESSLY SET FORTH ABOVE, TO THE EXTENT PERMITTED BY LAW, NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THIRD PARTY WARRANTIES, IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY OR SATISFACTORY QUALITY, OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY CA.

10.3. Customer warrants that (i) it has the right to transmit Customer Data and any data or information as may be required for the purposes of accessing SaaS, (ii) it is responsible for all activities that occur in user accounts, and (iii) it shall not misuse SaaS by sending spam or otherwise duplicative or unsolicited messages or store infringing, obscene, threatening, or otherwise unlawful material or material that is harmful to children or violates third party privacy rights.

11. WARRANTY REMEDY

11.1. If it is established that CA has breached the above warranty, CA may, at its option, (i) use reasonable efforts to cure the defect in the SaaS; (ii) replace the SaaS with SaaS that materially conforms to the specifications in the Documentation; (iii) in the event CA cannot, after commercially practicable attempts to do so, achieve the remedies in (i) or (ii), CA may terminate the subscription to the SaaS and provide

a refund of pre-paid, unused fees calculated against the remainder of the Subscription Term as of the effective date of such termination. Customer must report the alleged breach of warranty with reasonable specificity in writing within thirty (30) days of its occurrence to benefit from this warranty and the remedies stated herein. The above warranty remedies are CA's sole obligation and Customer's sole and exclusive remedy for breach of the above warranty.

12. SERVICE LEVEL COMMITTMENT

12.1. The Service Level Availability is measured against reports that CA conducts on a regular basis based on objective criteria. Reports are available to Customer upon request. If Customer cannot access SaaS during the Subscription Term, Customer should contact CA to receive SaaS Support.

12.2. If it is determined by Customer and confirmed by CA that SaaS is unavailable beyond the default threshold identified in the applicable SaaS Listing measured on a monthly basis during three contiguous months, then Customer has the right to elect any of the remedies specified therein.

12.3. The following events shall be excluded from the calculation of Service Level Availability: (i) Force Majeure Event; (ii) outages due to Scheduled Downtime; (iii) outages based on Customer networks or domain name server issues; (iv) Customer's configuration, scripting, coding drafted by Customer without CA's authorization or knowledge; (v) internet outages; (vi) outages requested by Customer; (vii) Customer changes to its environment which hinder SaaS production; (viii) outages to remedy a security vulnerability or as required by law and (ix) inability for Customer to log in to SaaS service because of dependence on non-CA provided services or components (*e.g.*, Lightweight Directory Access Protocol (LDAP) in Customer's environment).

13. GENERAL TERMS.

13.1. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the order of precedence set for in in Section 1.C. of Contract No. DIR-TSO-3793 The Parties have caused this SaaS Module to be executed by their duly authorized representatives as identified below.

Customer		**CA, Inc.**	
Signature:	_____	Signature:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date	_____	Date:	_____